FORM PTO-1390 (REV. 10-97) U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

# TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER: 00621/TL

U.S. APPLICATION NO. (If known, see 37 CFR 1.5): 09/646640

| INTERNATIONAL APPLICATION NO. | INTERNATIONAL FILING DATE | PRIORITY DATE CLAIMED |
|---|---|---|
| PCT/FR99/00613 | 17 MARCH 1999 | 17 MARCH 1998 |

TITLE OF INVENTION: METHOD FOR DATA SECUREMENT USING A CRYPTOGRAPHIC ALGORITHM

APPLICANT(S) FOR DO/EO/US: Patrick SALLE, a citizen of France

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. [X] This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371. 422 Rec'd PCT/PTO 18 SEP 2000
2. [ ] This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. [X] This express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
4. [X] A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. [X] A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. [ ] is transmitted herewith (required only if not transmitted by the International Bureau).
   b. [X] has been transmitted by the International Bureau.
   c. [ ] is not required, as the application was filed in the United States Receiving Office (RO/US).
6. [X] A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. [ ] Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. [ ] are transmitted herewith (required only if not transmitted by the International Bureau).
   b. [ ] have been transmitted by the International Bureau.
   c. [ ] have not been made; however, the time limit for making such amendments has NOT expired.
   d. [ ] have not been made and will not be made.
8. [ ] A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. [ ] An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. [ ] A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

**Items 11. to 16. below concern document(s) or information included:**

11. [X] An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. [ ] An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. [X] A FIRST preliminary amendment.
    [ ] A SECOND or SUBSEQUENT preliminary amendment.
14. [ ] A substitute specification.
15. [ ] A change of power of attorney and/or address letter.
16. [X] Other items or information:
    Form PCT/IB/308
    Form PCT/IB/409
    Form PCT/ISA/210

Express Mail Mailing Label No.: EL 615 575 271 US

Date of Deposit: September 18, 2000

I hereby certify that this paper and any papers identified herein is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231

Yolanda Usher

Yolanda Usher

| U.S. APPLICATION NO (If known, see 37 CFR 1.5) | INTERNATIONAL APPLICATION NO | ATTORNEY'S DOCKET NUMBER |
|---|---|---|
| 09/646640 | PCT/FR99/00613 | 00621/TL |

17. [X] The following fees are submitted:

| BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)): | | CALCULATIONS PTO USE ONLY |
|---|---|---|
| Search Report has been prepared by the EPO or JPO | $840.00 | |
| International preliminary examination fee paid to USPTO (37 CFR 1.482) | $670.00 | |
| No international preliminary examination fee paid to USPTO (37 CFR 1.482) but international search fee paid to USPTO (37 CFR 1.445(a)(2)) | $760.00 | |
| Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO | $970.00 | |
| International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(2)-(4) | $ 96.00 | |

| | | | | | |
|---|---|---|---|---|---|
| ENTER APPROPRIATE BASIC FEE AMOUNT = | | | | $ 840.00 | |
| Surcharge of $130.00 for furnishing the oath or declaration later than [ ] 20 [ ] 30 months from the earliest claimed priority date (37 CFR 1.492(e)). | | | | $ | |
| CLAIMS | NUMBER FILED | | NUMBER EXTRA | RATE | |
| Total claims | 8 | - 20 = | 0 | x$18.00 | $ 0 |
| Independent claims | 1 | - 3 = | 0 | x$78.00 | $ 0 |
| MULTIPLE DEPENDENT CLAIM(S) (if applicable) | | | | x$260.00 | $ |
| TOTAL OF ABOVE CALCULATIONS = | | | | | $ 840.00 |
| Reduction of 1/2 for filing by small entity, if applicable. Verified Small Entity Statement must also by filed (Note 37 CFR 1.9, 1.27, 1.28). | | | | | $ -- |
| SUBTOTAL = | | | | | $ 840.00 |
| Processing fee of $130.00 for furnishing the English translation later than [ ] 20 [ ] 30 months from the earliest claimed priority date (37 CFR 1.492(f)). + | | | | | $ -- |
| TOTAL NATIONAL FEE = | | | | | $ |
| Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). $40.00 per property + | | | | | $ |
| TOTAL FEES ENCLOSED = | | | | | $ 840.00 |
| | | | | Amount to be: refunded | $ |
| | | | | charged | $ |

a. [X] A check in the amount of $840.00 to cover the above fees is enclosed.

b. [ ] Please charge my Deposit Account No. _____ in the amount of $_____ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. [X] The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 06-1378. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

FRISHAUF, HOLTZ, GOODMAN, LANGER & CHICK, P.C.
767 Third Avenue - 25th Floor
New York, NY 10017-2023

Tel. No. (212) 319-4900
Fax No. (212) 319-5101

Thomas Langer
SIGNATURE

THOMAS LANGER
NAME

27,264
REGISTRATION NUMBER

Date: September 18, 2000

Attorney Docket No. 00621/TL

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

Applicant(s): Patrick SALLE

Serial No. : (National Phase of PCT/FR99/00613 filed on 17 Mar. 1999)

Filed : CONCOMITANTLY HEREWITH

For : METHOD FOR DATA SECUREMENT USING A CRYPTOGRAPHIC ALGORITHM

Art Unit :
Examiner :

Express Mail Mailing Label
No.: EL 615 575 271 US
Date of Deposit: September 18, 2000

I hereby certify that this paper is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Asst. Commissioner for Patents, Washington, D.C. 20231

Yolanda Usher

Yolanda Usher

**PRELIMINARY AMENDMENT**

Asst. Commissioner for Patents
Washington, D.C. 20231

S I R :

Please amend the above-identified application as follows:

IN THE ABSTRACT

Please replace the Abstract with the new Abstract appended hereto.

THE SPECIFICATION

Page 1, between lines 1 and 2, insert the heading

--FIELD OF THE INVENTION--.

Between lines 5 and 6, insert the heading

--BACKGROUND OF THE INVENTION--.

Page 2, between lines 3 and 4, insert the heading

--SUMMARY OF THE INVENTION--.

Between lines 25 and 26, insert the heading

--BRIEF DESCRIPTION OF THE DRAWING--.

Between lines 31 and 32, insert the heading

--DETAILED DESCRIPTION OF THE DRAWING--.

Page 3, line 1, after the period insert --A description of the algorithms used in DES is presented in the document Federal Information Processing Standards Publication 46-2, Dec. 30, 1993 issued by the National Bureau of Standards, and its content is hereby incorporated by reference.--

line 19, delete "random".

IN THE CLAIMS

Please amend claims 3, 4, 5, 7 and 8 as follows:

Claim 3, line 1, change "either of claims 1 or 2" to --claim 1--.

Claim 4, line 1, change "any of claims 1, 2 or 3" to --claim 1--.

Claim 5, line 1, change "any of the preceding" to

--claim 1,--.

line 2, delete "claims,".

Claim 7, line 1, change "any of the preceding" to

--claim 1,--.

line 2, delete "claims,".

Claim 8, line 1, "any of the preceding" to

--claim 1,--.

line 2, delete "claims,".

Respectfully submitted,

Thomas Langer
Reg. No. 27,264

Frishauf, Holtz, Goodman, Langer & Chick, P.C.
767 Third Avenue - 25th Floor
New York, New York 10017-2032
Tel. (212) 319-4900
Fax (212) 319-5101
TL:yu

# METHOD FOR DATA SECUREMENT USING A CRYPTOGRAPHIC ALGORITHM

The present invention relates to a data protection method, for example designed to be implemented by the microprocessor of a bank card or an access authorization card during a connection to an authenticating computer terminal.

The known types of data protection methods use a cryptographic algorithm comprising execution cycles of repetitive operations for processing data elements contained in a memory of the card so as to generate encrypted information intended to be communicated to the computer terminal.

The execution of the method by the microprocessor of the card results in the sending of derivative signals such as peaks in the level of the microprocessor's electric power consumption, or variations in the electromagnetic radiation such that the envelope of electromagnetic radiation is indicative of the data processed. An attacker seeking to use the microprocessor cards in an unauthorized way can trigger the execution of the method repeatedly and analyze the derivative signals emitted in order to determine correspondences between the various processing operations and each signal or series of signals. From these correspondences, and for example by subjecting the card to electromagnetic disturbances or voltage drops at precise moments in the execution of the algorithm, the attacker can study the encrypted information obtained and the differences, or lack of differences, between the derivative signals emitted, in order to discover the data contained in the memory of the card.

To complicate this type of analysis of the derivative signals, it has been suggested that parasitic signals be generated and added to the derivative signals emitted during the execution of the method. The extraction of the signals that correspond to the execution of the method is then more difficult, but it is still possible. It has also been suggested that the electronic components of the card and the program for executing the method be designed so that the derivative signals emitted are

independent of the value of the sensitive data. However, this complicates the production of the cards without providing satisfactory protection of the data.

One object of the invention is to offer an effective protection method that does not have the aforementioned disadvantages.

In order to achieve this object, the invention provides a data protection method using a cryptographic algorithm for executing operations for processing data elements so as to generate encrypted information, this method comprising at least one step for the random transformation of the execution of at least one operation from one cycle to another, or for the random transformation of at least one of the data elements, so that the encrypted information is unchanged by this random transformation.

Random transformation of the execution of at least one operation is intended to mean a modification of the order of execution of operations or parts of operations, or a modification of the execution of a single operation. Thus, at least one operation and/or at least one of the pieces of data processed is randomly modified, which randomly affects the derivative signals emitted. This makes it very difficult for an attacker to distinguish between the various processing operations and to discover the data from the derivative signals. Moreover, the random modification does not affect the encrypted information, so it can be used in the normal way after it is generated.

Other characteristics and advantages of the invention will emerge through the reading of the following description of a particular non-limiting embodiment of the invention, in connection with the single attached figure, illustrating in the form of a block diagram the execution of the method according to this embodiment.

The protection method according to the invention described herein uses a symmetric cryptographic algorithm of the DES (DATA ENCRYPTION STANDARD) type to generate 64-bit encrypted information C from a message block M and a secret key K1, both

64-bit.

The method begins with the permutation 10 of the bits of the message block M with one another, in order to form the block M0.

The block M0 is then divided into two 32-bit blocks M1 and M2 during a division step 20.

It then performs the expansion 30 of the block M2 to form a 48-bit block M3. This expansion 30 is performed, for example, by partitioning the block M2 into eight quartets, and by adding to each quartet the adjacent end bit of the quartets framing the quartet in question (the end quartets being considered to be adjacent).

In parallel with these operations, a permutation 110 is performed on the bits of the key K1 to form the key K2. The insignificant bits of the key K1 are simultaneously deleted so that the key K2 has only 56 bits.

According to the invention, the bits of the key K2 are then randomly modified during a transformation 120. The bits of the key K3 corresponding to the modified bits of the key K2, here marked with a star, are stored. The random transformation 120 is for example performed by associating with the key K2, by means of a logical operator of the exclusive-OR type, a random number generated by an unpredictable number generator of the card.

A key K4 is obtained through the rotation 130 of the bits of the key K3. Then, a permutation 140 is performed on the bits of the key K4 to form the key K5. Simultaneously with the permutation 140, the insignificant bits of the key K4 are eliminated so that the key K5 comprises 48 bits.

The method continues with the association 210 of the block M3 and the key K5 by means of a logic operator of the exclusive-OR type. The result of this association is the block R1.

The inverse transformation of the bits of the block R1 corresponding to the bits modified by the transformation 120 is then performed in order to form the block R2. The purpose of this inverse transformation 220 of the transformation 120 is to return the bits of the block R1 corresponding to the bits marked with a

star to the state in which they would have been without the transformation 120.

The method then continues, in a conventional way, with the division and the processing 230 of the block R2, the permutation 240 of the bits of the block R3 formed in step 230, and the association 250 of the block R4 resulting from step 240 with the block M1 by means of an exclusive-OR operator, in order to form the block R5.

The group of operations designated overall by the reference 270 is then re-executed five times assigning, with each execution, the value of the block M1 to the block M2 and the value of the block R5 to the block M1 during an assignment step 260.

The method ends with the operation 300 for obtaining the encrypted information C through the inverse permutation and the combining of the last block M2 and the last block R5 obtained.

It is understood that the step for randomly modifying the key K2 comprises the transformation phase 120 and the inverse transformation phase 220. These two phases make it possible to obtain encrypted information C that is not affected by this random modification.

It would also be possible, in the same way, to perform a random modification of the block M2 and/or of another piece of data.

According to another embodiment of the invention, which can be associated with a modification step like the one described above, the execution of at least one operation can be randomly modified from one cycle to another, a cycle being a complete execution cycle of the algorithm or an intermediate execution cycle of a group of operations.

For example, a random determination of the order of execution of certain operations can be made during an execution cycle of the algorithm. The operations retained are the ones whose order of execution relative to the others does not affect the result. To make this determination, it is possible to

perform, at the end of the chosen operations, a conditional jump to certain operations as a function of the value of a random number or to define a table of the addresses of the various operations, scanned randomly.

For example, the permutation 10 of the bits of the message block M could be performed after the permutation 110 of the bits of the key K1, or vice versa.

Likewise, it is possible to provide for a random determination of the order of execution of the operations of the group 270 for each intermediate execution cycle of the latter (16 intermediate execution cycles of these operations for one complete execution cycle of the algorithm). Here again, the order of execution of these operations is chosen so as not to affect the result.

Furthermore, for certain operations, the data are processed in elements. Thus, during the expansion 30, the blocks M2 are processed in quartets. During this operation, it is possible to provide for a random determination of the processing order of the various quartets. Likewise, during the permutation 140, the bits of the key K4 are processed individually. A step for randomly determining the processing order of the bits can also be provided for the execution of this permutation. The quartets of the block M2 can also be processed alternately with the bits of the key K4, meaning for example that a first quartet of the block M2 is processed, followed by a bit string of the key K4, followed by a second quartet of the block M2, etc., each time storing the data elements processed in order to verify that all of the required operations are actually executed.

Of course, the invention is not limited to the embodiment just described, but on the contrary encompasses any variant that retains, with equivalent means, its essential characteristics.

In particular, although the invention has been described in connection with an algorithm of the DES type, the invention can be applied to other symmetric algorithms that work by modifying bits. Thus, the modification being performed by means of a

logical operator of the exclusive-OR type, the length of the non-transformed data elements is identical to the length of these data elements transformed.

Furthermore, the numbers of bits of the data are only mentioned as an example and can be modified in order to be adapted to the degree of protection sought.

It will also be noted that all of the data elements M, M0, M1, M2, M3, K1, K2, K3, K4, K5, R1, R2, R3, R4 and R5 can be transformed by associating a random number with them, by means of the exclusive-OR logical operator, bearing in mind that after this random transformation step, an inverse transformation step is performed so that the encrypted information C is unchanged by said transformations.

In particular, the data elements can be keys K1, K2, K3, K4, K5 or message blocks M, M0, M1, M2, M3, or message blocks associated with a key by a logical operator of the exclusive-OR type R1, R2, R3, R4, R5.

Finally, it will be noted that if the random transformation step is a step that precedes the group of operations executed repeatedly, and if the inverse transformation step is a step that follows said group of operations, generating a random number once and processing the message block M with the algorithm is enough to obtain the encrypted information, all the data elements of the block being modified. The data string is protected from end to end. Moreover, by not multiplying the transformation steps and the number of random numbers generated, the algorithm is executed quickly, which is necessary in the case of a chip card, in which the execution time of an algorithm should be minimal.

## CLAIMS

1. Data protection method (M) using, in a microprocessor of a chip card, a cryptographic algorithm for executing operations for processing data elements (M, M0, M1, M2, M3, K1, K2, K3, K4, K5, R1, R2, R3, R4, R5) so as to generate encrypted information (C), characterized in that it comprises at least one step for the random transformation (120) of bits of at least one of the data elements (K2) by associating a random number with said data element (K2) by means of a logical operator of the exclusive-OR type, and after this random transformation step, an inverse transformation step (220) such that the encrypted information (C) is unchanged by these transformation steps (120, 220).

2. Protection method according to claim 1, characterized in that a randomly transformed data element is a key (K1, K2, K3, K4, K5).

3. Protection method according to either of claims 1 or 2, characterized in that a randomly transformed data element is a message block (M, M0, M1, M2, M3).

4. Protection method according to any of claims 1, 2 or 3, characterized in that a randomly transformed data element is a message block associated with a key by a logical operator of the exclusive-OR type (R1, R2, R3, R4, R5).

5. Protection method according to any of the preceding claims, characterized in that the cryptographic algorithm for executing operations for processing data (M, M0, M1, M2, M3, K1, K2, K3, K4, K5, R1, R2, R3, R4, R5) comprises a group of operations (270) executed repeatedly.

6. Protection method according to claim 5, characterized

in that the random transformation step is a step that precedes the group of operations (270) executed repeatedly and in that the inverse transformation step is a step that follows said group of operations (270).

7. Protection method according to any of the preceding claims, characterized in that it also comprises a step for randomly modifying the order of execution of the operations of the group of operations (270).

8. Protection method according to any of the preceding claims, characterized in that the cryptographic algorithm is the DATA ENCRYPTION STANDARD type.

**ABSTRACT**

The invention relates to a data protection method using a cryptographic algorithm comprising at least one execution cycle of repetitive operations for processing data elements (K2, R1) so as to generate encrypted information (C), this method comprising at least one step (120, 220) for randomly modifying the execution of at least one operation from one cycle to another, or at least one of the data elements, so that the encrypted information is unchanged by this random modification.

## ABSTRACT OF THE DISCLOSURE

A data protection method using a cryptographic algorithm comprising at least one execution cycle of repetitive operations for processing data elements (K2, R1) so as to generate encrypted information (C). At least one step (120, 220) is provided for randomly modifying the execution of at least one operation from one cycle to another, or at least one of the data elements, so that the encrypted information is unchanged by this random modification.

Attorney Docket No. 00621/TL



CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, D C 20231, on the date noted below

Attorney: Thomas Langer

Dated: November 6, 2000

In the event that this Paper is late filed, and the necessary petition for extension of time is not filed concurrently herewith, please consider this as a Petition for the requisite extension of time, and to the extent not tendered by check attached hereto, authorization to charge the extension fee, or any other fee required in connection with this Paper, to Account No. 06-1378.

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

Applicant(s): Patrick SALLE

Serial No. : 09/646,640

Deposited : September 18, 2000

For : METHOD FOR DATA SECUREMENT USING A CRYPTOGRAPHIC ALGORITHM

Art Unit :
Examiner :

**LETTER TO OFFICIAL DRAFTSPERSON**

BOX MISSING PARTS
Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

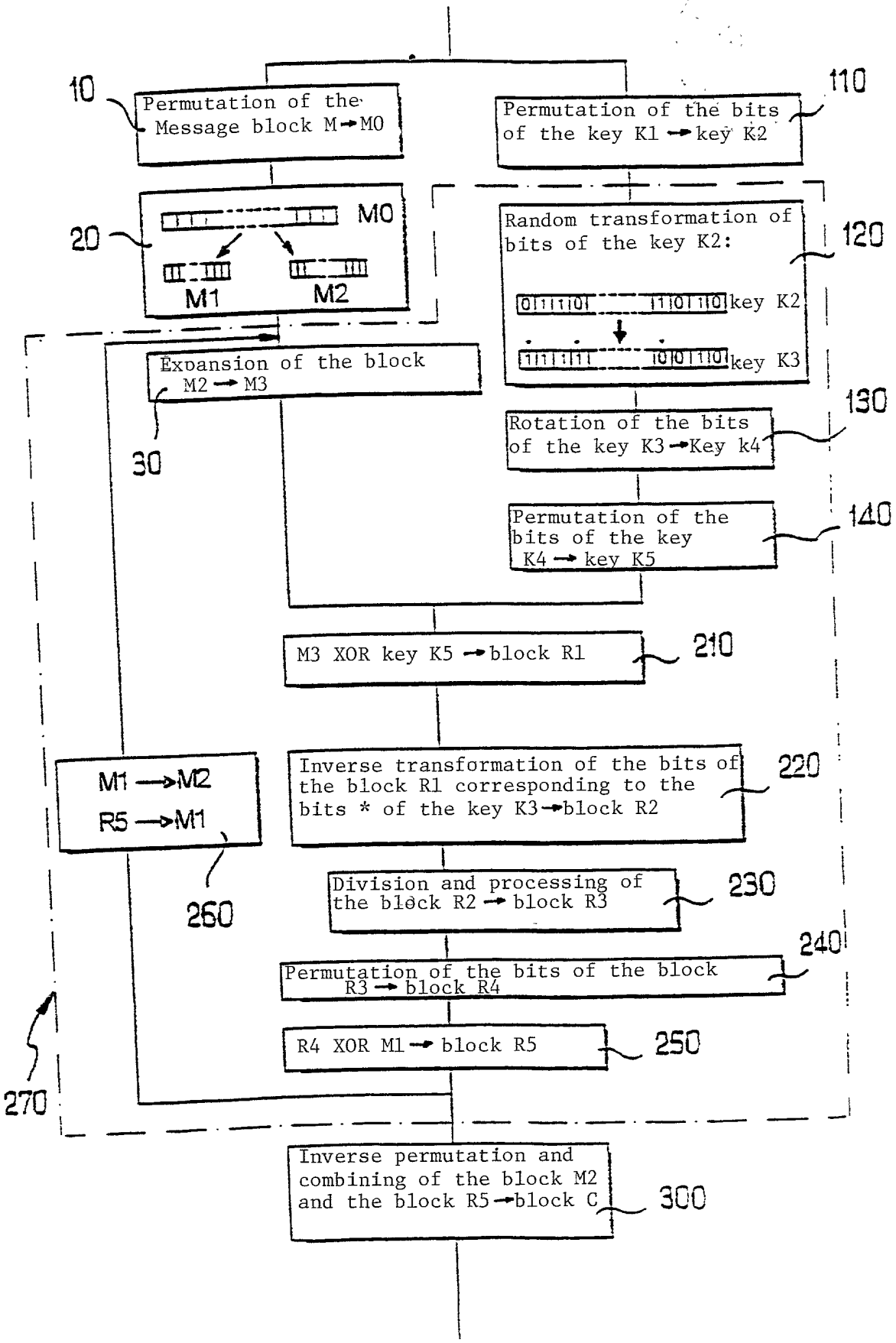
Submitted herewith is one sheet of drawing showing the English translation of the original French labeling for the boxes in the drawing. No new matter is involved.

Approval and entry is respectfully requested.

Respectfully submitted,

Thomas Langer
Reg. No. 27,264

Frishauf, Holtz, Goodman, Langer & Chick, P.C.
767 Third Avenue (25th Floor)
New York, New York 10017-2023
Tel. No. (212) 319-4900
Facsimile (212) 319-5101
TL:yu


10
Permutation of the Message block M → M0
110
Permutation of the bits of the key K1 → key K2
20
M0
M1
M2
Random transformation of bits of the key K2:
120
key K2
key K3
Expansion of the block M2 → M3
30
130
Rotation of the bits of the key K3 → Key k4
140
Permutation of the bits of the key K4 → key K5
M3 XOR key K5 → block R1
210
M1 → M2
R5 → M1
260
Inverse transformation of the bits of the block R1 corresponding to the bits * of the key K3 → block R2
220
Division and processing of the block R2 → block R3
230
240
Permutation of the bits of the block R3 → block R4
R4 XOR M1 → block R5
250
270
Inverse permutation and combining of the block M2 and the block R5 → block C
300

9/97FHGL&C

U.S. Attorney Docket 00621/TL



# APPLICATION FOR UNITED STATES LETTERS PATENT

## POST-FILED PCT Declaration and Power of Attorney (35 U.S.C. 371(c)(4))
## PCT Application - United States Designated Office

As a below named inventor, I declare that:

My residence, post office address and citizenship are as stated below next to my name; I believe that I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

**METHOD FOR DATA SECUREMENT USING A CRYPTOGRAPHIC ALGORITHM**

described and claimed in International Application number PCT/FR99 /00613 filed 17 March 1999

I have reviewed and understand the contents of said specification, including claims.
I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR §1.56.

I claim priority benefits under 35 USC §119 of: (i) any foreign application(s) for patent or inventor's certificate listed below; or (ii) any United States provisional application(s) listed below; and have also identified below any foreign application(s) for patent or inventor's certificate, or PCT international application having a filing date before that of the application(s) on which priority is claimed.

| COUNTRY | APPLICATION NUMBER | DATE (day, month, year) | PRIORITY CLAIMED |
|---|---|---|---|
| FRANCE | 98/03242 | 17 MAR. 1998 | yes X no |
| | | | yes no |

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

I appoint the following attorneys to prosecute this application and to transact all business in the U.S. Patent & Trademark Office connected therewith: Leonard Holtz, Reg. No. 22,974; Herbert Goodman, Reg. No. 17,081; Thomas Langer, Reg. No. 27,264; Marshall J. Chick, Reg. No. 26,853; Richard S. Barth, Reg. No. 28,180; Douglas Holtz, Reg. No. 33,902; and Robert P. Michal, Reg. No. 35,614.

CORRESPONDENCE AND CALLS TO:

FRISHAUF, HOLTZ, GOODMAN, LANGER & CHICK, P.C.
767 Third Avenue - 25th Floor
New York, New York 10017-2023
Tel.: (212) 319-4900
Fax.: (212) 319-5101

| INVENTOR: SIGNATURE | DATE | RESIDENCE AND POST OFFICE ADDRESS |
|---|---|---|
| Sign: P Salle | Date: 9 Octobre 2000 | Residence: (City & Country) VERRIERES LE BUISSON, FRANCE FRX<br>Post Office Address: 46, rue d'Amblainvilliers 91370 Verrieres Le Buisson, France |
| Type: Patrick SALLE | Citizen of: FRANCE | |
| Sign: | Date: | Residence: (City & Country)<br>Post Office Address: |
| Type: | Citizen of: | |
| Sign: | Date: | Residence: (City & Country)<br>Post Office Address: |
| Type: | Citizen of: | |